ST. JOHN'S C OF E

LIVING, LOVING LEARNING

PRIMARY SCHOOL

Policy for E-safety

Last Reviewed by Governing Body : Feb 2018

Date of next review : Feb 2020

Mission and Vision Statement

Our mission is that:

Each of us is special; each of us is unique.

We aim to provide pupils with high quality teaching and learning, so that they can become effective life-long learners, striving for excellence.

We aim to demonstrate clear Christian characteristics and values, whilst at the same time, encouraging recognition of and respect for other faiths.

We value greatly school, home and parish connections.

We believe in "Living, Loving and Learning" together in God's World.

Our vision is to:

Empower creative independent thinkers, who are resilient to challenges, in readiness for our diverse and ever-changing world.

Introduction

This document is a statement of the aims and effective approaches to e-safety at St John's C.E. School.
Safeguarding children, including e-safety is everyone`s responsibility.

School E-Safety Policy

Safeguarding children, including e-safety is everyone`s responsibility. The Heads of Sites are the designated persons for Child Protection and therefore is responsible for e-safety. This role will overlap with the role of the ICT subject leader, and the ICT Technician, and they will work collaboratively to ensure ever-changing issues relating to the Internet and its safe use are addressed. The policy will be reviewed regularly and changes will be made immediately if technological or other developments so require.

What is E-Safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Child Protection, I.C.T, P.S.H.E, Positive Behaviour and Anti-Bullying, Teaching and Learning, Data Protection and Security.

The aim of this policy is to clarify roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies and to ensure that existing policies (Child Protection, I.C.T, P.S.H.E, Positive Behaviour and Anti-Bullying, Teaching and Learning, Data Protection and Security) are applied to the digital environment.

Managing the use of on-line technology

At St John`s the e-safety leads are Louise Bonter (Head of Infant Site) and Chris Gibson (Head of Junior Site) who are also the designated persons for Child Protection

The responsibilities of the lead person include :

- Updating the E-safety and Acceptable Use Policy
- Ensuring that policies and procedures include aspects of e-safety, for example cyber-bullying is included in the anti-bullying policy and the Child Protection policy includes child grooming and sexting.
- Working with the IT technicians from Failsworth Sports College to ensure that the filtering is set at the correct level for staff and children and inappropriate language or images.
- Ensure staff training is provided on e-safety issues
- Ensure that e-safety is included in induction
- Monitor and evaluate incidents that occur to inform safeguarding developments

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband ensuring effective management of content filtering.
- National Education Network standards and specifications.

Educational benefits of the Internet

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils world-wide.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system update.
- Access to tools of direct communication such as Video conferencing and email.
- Exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

Principles of the teaching and learning of e-safety

The purpose of using on-line technology in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school`s management information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils including the blocking of any extremist material and inappropriate language or images.

In addition to using the internet in school, we recognise that children will use the internet and other digital technology in their own time at other locations and are at greater risk if they have not been taught what the dangers are and how to use them safely. Supporting and assisting the development of children`s e-confidence and their ability to access the digital world effectively and safely is essential.

We acknowledge that the range of risks to young people in the digital environment is wide and ever changing e.g "grooming" by sexual predators via internet-enabled multi-player games is not uncommon.

At St John`s, we recognise the importance of raising the awareness of children so that they are able to keep themselves as safe as possible when using the internet and other digital technologies. In order to do this, we involve children and their parents/carers in the safe use of on-line technologies. Children are taught what on-line technology use is acceptable and what is not and are given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval. Lessons on e-safety are delivered on a regular basis and our local PCSOs and LA provide input and scenarios regarding e-safety for the children to consider.

If staff or pupils discover unsuitable sites the URL (address) and contents must be reported to the Internet Service provider via the ICT co-ordinator. The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

We provide support and guidance to pupils and their parents/carers for the safe and responsible use of these on-line technologies. A partnership approach with parents is encouraged and guidance regarding e-safety is offered to parents in variety of different ways e.g information events, relevant links and documents available on the school website.

Acceptable Use

In order to prevent inappropriate situations occurring, it is important that staff, volunteers and children are aware of their responsibilities and the expectations whilst using technology. Each user signs a contract to ensure they know what is deemed "acceptable use of the internet"

Password security

Password security is essential for staff as they are able to access and use pupil data. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and MIS. Staff should ensure that computers and laptops are not left unattended.

Internet access

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form giving permission for their child to use the internet.

In Foundation Stage and Key Stage 1, access to the internet is by adult demonstration and direct supervised access to specific, approved on-line materials.

In Key Stage 2, pupils use the internet for research purposes in addition to specific tasks. Pupils are taught the importance of e-safety and agree terms and conditions for acceptable internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may not always be reliable or accurate.

E-mail

Children may only use approved e-mail accounts on the school system. Children use class accounts that are restricted to communication within the school, within the school`s virtual learning environment. Children must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet someone. Children are instructed to tell an adult if they receive an offensive e-mail. E-mails sent to external organisations should be carefully written and authorised before sending, in the same way as a letter written on school headed notepaper. The forwarding of chain letters is not permitted. Access in school to external personal e-mail accounts may be blocked. Passwords should be secure on the L.A. First class System

School website

The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils` home information will not be published. Website photographs that include pupils will be selected carefully. Pupils` full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents/carers will be obtained before photographs of pupils are published on the school website. The Head Teacher will take overall editorial responsibility and ensure content is accurate and appropriate.

Chat and instant messaging

Staff and pupils will not be allowed access to public or unregulated chat rooms. Pupils will not access social networking sites e.g. “Instagram”, “Snapchat”, “My Space””, “Bebo”, “Facebook.” Pupils will only be allowed to use regulated educational chat environments such as those in the VLE. This will be supervised and the importance of chat room safety emphasised. Any forms of bullying or harassment is strictly forbidden and will be dealt with in line with the school`s behaviour policy. To keep pupils safe at home, pupils are advised not to place personal photos on any social network space. Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.

Photographic, video and audio technology

It is not appropriate to use photographic or video devices in changing areas or toilets. Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed. Staff may use photographic or video devices (including digital cameras, IPads and mobile phones) to support school trips and curriculum activities. The downloading of audio and video files is not permitted without the prior permission of the e-safety lead and only in cases where they relate directly to the current educational task being undertaken. Pupils should always seek permission of their teacher before making audio, photographic or video recordings within school grounds.

Video Conferencing

- IP videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils are not permitted to use the Videoconferencing equipment unsupervised.
- Equipment needs to be switched off when not in use.
- The address should not be made available to other sites.
- Contact must be established with other conference participants before taking part in videoconferencing to ensure the material delivered is appropriate for the class.

Emerging ICT applications

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Emerging applications are encouraged to enhance learning and will be used in accordance with this policy. Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff will be issued with a school phone where contact with pupils is required.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessment of risk

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Oldham LA can accept liability for material accessed or any consequences of internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. The Head Teacher will ensure that the e-safety policy and Acceptable Use Policy is implemented and compliance with the policy is monitored.

Filtering

The school will work in partnership with parents, the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. The filtering strategy is selected to suit the age and curriculum requirements of the pupils, including the blocking of extremist material and inappropriate language or images.

Introducing the policy to pupils

- Rules for acceptable use will be posted in all rooms where computers are used.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- A lesson on responsible internet use covering both school and home use should be delivered each time equipment is used.

Introducing the policy to staff and volunteers

- All staff and volunteers must accept the terms of responsible internet usage before using any internet resource in school.
- All staff including teachers, supply staff, classroom assistants, administration, caretaking staff and Governors will be provided with the School Internet policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the SLT.
- Staff development in safe and responsible Internet use, including familiarisation of the e-safety and acceptable use policy will be provided as required.

Introducing the policy to parents

- Parents' attention will be drawn to the School e-Safety Policy in Newsletters, the School Prospectus and on the School Web site.
- Parent's need to give permission for children to use the Internet.
- Parents need to give permission to have any photographs published of their children on the Website.

Maintaining ICT system security

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.

- Personal data sent over the internet will be encrypted or otherwise secured. All personal devices will be encrypted by the ICT team.
- Each member of the teaching staff has been given a personal portable USB device which is encrypted with password protection; this allows for safe use.
- Unapproved system utilities and executable files will not be allowed in pupils` work areas or attached to e-mail.
- Files held on the school`s network and the cloud will be regularly checked.
- The ICT Leader/ICT technicians will ensure that the system has the capacity to take increased traffic caused by internet use.

The responses necessary when a risk to a child is discovered

Prompt action is required if a complaint is made regarding the use of on-line technology. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Oldham LSCB child protection procedures.

Any complaints regarding staff misuse must be referred directly to the Head Teacher.

Equal Opportunities

Provision is made for all children regardless of ability, disability, additional needs, medical conditions, gender, faith or ethnicity and reasonable adjustments are made in a range of ways. All children have a right to be treated equally and the school will take measures against those who do not abide by this ethos.

Monitoring and Evaluation

Policy and practice is monitored and evaluated on a regular basis. Monitoring may take the form of lesson observations, planning, questionnaires, discussions with children or learning walks. Feedback will be given to all staff along with recommendations to inform future policy and planning.
The school leadership team have a responsibility to ensure the policy is embedded into the school provision and report to governors on the effectiveness of the policy.

How to respond if a risk is discovered

The e-safety lead will ensure that an adult follows these procedures in the event of any misuse of the internet :

An inappropriate website is accessed inadvertently :

- Report website to the e-safety lead.
- Contact the filtering service so that the site can be added to the banned or restricted list.
- Change local control filters to restrict locally.
- Log the incident.

An inappropriate website is accessed deliberately :

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the Head Teacher and e-safety lead immediately.
- Head Teacher to refer to Acceptable Use Rules and follow agreed actions for discipline.
- Inform the filtering services in order to reassess the filters.

An inappropriate website is accessed deliberately by a child or young person :

- Refer to the Acceptable Use rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and that the police can be informed.
- Log the incident.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Contact the filtering to notify them of the website.

An adult receives inappropriate material :

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Head Teacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g police, social services, CEOP.
- Log the incident.

An illegal website is accessed or illegal material is found on a computer. (The following incidents must be reported directly to the police)

- Indecent images of children found. (Images of children whether they are cartoons of children or young people apparently under the age of 16 involved in sexual activity or posed in a sexually provocative manner)
- Incidents of “grooming” behaviour.

- The sending of obscene materials to a child.
- Criminally racist or anti-religious material.
- Violent or bomb making material.
- Software piracy.
- The promotion of illegal drug taking.
- Adult material that potentially breaches the obscene publications act in the UK.

If any of these are found, the following should occur :

- Alert the Head Teacher/e-safety lead immediately.
- DO NOT LOG OFF the computer but disconnect from the electricity supply.
- Contact the police and or CEOP and social care immediately.
- If a member of staff or volunteer is involved, refer to the allegations made against staff guidelines in the Child Protection Policy and report to the Local Authority Designated Officer.

An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text messages etc)

- Ensure the child is reassured and remove them from the situation.
- Report to the manager and Designated Person for Child Protection immediately who will then follow the Allegations procedure and child protection procedures.
- Report to the Local Authority Designated Officer.
- Preserve the information received by the child if possible.
- Contact the police as necessary.

Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school :

- Preserve any evidence and log the incident.
- Inform the Head Teacher immediately and follow Child Protection policy.
- Inform the e-safety lead so that new risks can be identified.
- Contact the police or CEOP as appropriate.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Head Teacher.

Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

- Preserve any evidence and log the incident.
- Inform the Heads of Site or e-safety leader immediately.
- Check the filter if an internet based website issue.
- Contact parent/carers.
- Refer to the anti-bullying policy.
- Contact the police or CEOP as necessary.